

REMARKS/ARGUMENTS

In reply to the Office Action dated August 30, 2004, please enter the above-listed amendments and consider the following remarks. By way of this response, Applicants amend claims 1, 7-8, 11-14, 16, 19-22, and 29-32, and cancel claims 35-38 and 40-41 without prejudice or disclaimer. After entry of this paper, claims 1-8, 10-34, 39, and 42-47 will be pending in this application.

112 Rejections

At Paragraph 2, the Office Action rejected Claims 1-6, 29, and 31-33 under 35 USC 112, stating "it is unclear what qualifies the client for the key." Claim 1 has been amended to recite, "receipt of said ticket to qualify the receiving client to access a key from the key server upon presentation of information derived from the ticket to the key server." Support is found in the present specification, for example, at page 10, lines 6-7, where it is indicated that a digital hash on the ticket may certify that the client is authorized to access a key for any of the listed events. Dependent Claims 2-6 are believed to be likewise clarified in view of the amendment to Claim 1. Similar clarifying amendments have been presented for Claims 29, 31, and 32. Dependent Claim 33 is believed to be clarified in view of the amendment to Claim 32. Accordingly, Applicants request that the instant rejections under 35 USC 112 be withdrawn and the claims allowed.

103 Rejections

At Paragraph 4, the Office Action rejected Claims 1-3, 5-8, 10, 13, 16-23, 26, 29, 32-33, 35, 38, and 42-47 under 35 USC 103(a) as being unpatentable over Akins III et al., U.S. 6,744,892 ("Akins"). At Paragraph 5, the Office Action rejected Claims 11-12, 14-15, 24-25, 27-28, 34, 36-37, 39-41, and 48 under 35 USC 103(a) as being unpatentable over Akins in view of Schmeidler et al., U.S. 6,763,370 ("Schmeidler"). For clarity, the pending claims will be addressed in numerical order, with Paragraphs 4 and 5 of the Office Action being referenced as appropriate.

Claim 1

For several reasons, it is respectfully submitted that Claim 1, as amended, is patentable over Akins. First, as noted in the Office Action, Akins does not disclose a "multicast" as recited

in Claim 1. Rather, Akins discusses a cable television distribution system which, at least by virtue of the concentrated content delivery system in which all encrypted program information flows from a "headend 515", represents a substantially different field of endeavor than a multicast environment with respect to security and access issues. Nevertheless, Claim 1, as amended, would not be suggested by Akins regardless of the many distinctions between cable television and multicast scenarios, as explained herein.

Akins discloses the broadcast transmission of encrypted instances 105, the encrypted instances 105 comprising both encrypted instance data 109 and Entitlement Control Messages (ECMs) 107 (FIG. 1; col. 4 lines 34-39). The encrypted instance data 109 is encrypted at or behind the "headend 515" using a symmetric Control Word (CW) 202 that is changed once every few seconds (col. 6 lines 41-43). Each ECM 107 contains a symmetrically encrypted version of the CW (col. 6, lines 55-57), which must therefore be decrypted at the set-top-box 113 before the CW can be used to decrypt the encrypted instance data 109. The CW is encrypted using a symmetric Multi-Session Key (MSK) 205 (col. 6, line 58-60). An asymmetrically encrypted copy of the MSK is provided to the set-top box 113 encapsulated within an Entitlement Management Message (EMM) 111. In particular, the MSK is encrypted to the public key of the set-top-box 113 (col. 6, line 64- col. 7, line 1). The set-top box 113 then uses its private key to decrypt the encrypted MSK, which in turn is used to decrypt the encrypted CW, which in turn is used to decrypt the encrypted instance data 109.

First, Akins does not teach or suggest "the receiving client to access a key from a key server . . . wherein the key is a symmetric key that the sending client uses to encrypt the multicast event and the receiving client uses to decrypt the multicast event" as recited in Claim 1, as amended. In Akins, the "symmetric key that the sending client uses" is the CW, whereas the set-top box receives an *encrypted version* of the CW from the broadcast transmission, and *separately* receives the MSK key in the EMM message. The set-top box must locally generate the CW by itself, each and every time the CW changes (every few seconds), and does not receive the CW from a key server. Accordingly, the set-top box does not access a key from a key server that is "a symmetric key that the sending client uses to encrypt the multicast event."

Second, claim 1 has been amended to recite,

"the symmetric key being refreshed at relatively short intervals compared to a duration of the multicast event, the refreshed symmetric keys being transmitted from the key server to said receiving client during the multicast event"

Importantly, the only symmetric key in Akins that might be characterized as being "refreshed at relatively short intervals compared to a duration of the event" is the CW, which is refreshed every few seconds. However, as explained above, the CW is not "transmitted from the key server to said receiving client." Moreover, the MSK key of Akins is not taught or suggested as being "refreshed at relatively short intervals compared to a duration of the event" as recited in Claim 1, as amended. In particular, Akins states at col. 6, lines 60-61, "The MSK lifetime is typically hours or days in length," and no described relationships of MSK lifetime with event durations could be found. It is to be further appreciated that the MSK key is not a "key that the sending client uses to encrypt the multicast event," because the MSK encrypts the CW and not the instance data content itself.

Claims 2-3 are submitted to be allowable for at least the reason that they depend from an allowable base claim.

Claim 4 was not rejected under 35 USC 103(a). See above discussion of 35 USC 112 Rejections.

Claim 5 is submitted to be allowable for at least the reason that it depends from an allowable base claim.

Claim 6 is submitted to be allowable for at least the reason that it depends from an allowable base claim. Furthermore, it could not be found in the Akins portions cited in the Office Action (cols. 4-5, col. 22, lines 30-60, col. 23, col. 27, lines 1-10) "wherein the list comprises . . . an internet protocol (IP) address for each listed event . . . and an IP address for a key server corresponding to each listed multicast event." Instead, as understood, Akins discusses a cable TV distribution system, with the set-top box only getting content that passes through the "headend 515."

Claim 7

It is respectfully submitted that Claim 7, as amended, is patentable over Akins for reasons similar to those presented above in regard to Claim 1. For example, Akins does not

teach or suggest "at relatively short intervals compared to a duration of the multicast event, transmitting refresh keys to the receiving client, each refresh key being a symmetric key that the sending client uses to encrypt the multicast event and the receiving client uses to decrypt the multicast event" as recited in Claim 7, as amended. Various other minor amendments have been made to Claim 7 for further clarity, antecedent basis, etc.

Claim 8, as amended for consistency with amended Claim 7, is submitted to be allowable for at least the reason that it depends from an allowable base claim.

Claim 9 was previously canceled.

Claims 10-11 are submitted to be allowable for at least the reason that they depend from an allowable base claim. Claim 11 has been amended for consistency with amended Claim 7.

Claim 12 was rejected under 35 USC 103(a) as being unpatentable over Akins in view of Schmeidler. Although submitted to be allowable for at least the reason that it depends from an allowable base claim, it is further noted that (i) there would be no motivation to reference the teachings of Schmeidler in relation to the problems posed by a multicast environment, and (ii) Schmeidler does not teach or suggest "said particular time being randomly generated by the receiving or sending client for a first forward security window and applied for each forward security window thereafter," as recited in Claim 12, as amended.

First, Schmeidler discusses an "on-demand" content delivery system in which content is *separately* downloaded from a Random Access File Transfer (RAFT) server 205 to each individual user PC in a point-to-point manner. This is a substantially different environment than a multicast environment, because Schmeidler's separate download processes, which are generally initiated by different users at different times ("on-demand") would be naturally staggered in time and there would be little or no traffic peak problems in receiving permission refresh requests. Accordingly, there would be no motivation to reference the teachings of Schmeidler in relation to the different problems posed by a multicast environment.

Second, it could not be found in Schmeidler "said particular time being randomly generated by the receiving or sending client for a first forward security window and applied for each forward security window thereafter," as recited in Claim 12, as amended. As understood,

Schmeidler discusses an initial web purchase by the user (col. 9, lines 5-20), and then discusses refresh requests "periodically" for the "activator" (col. 9, line 68 – col. 10, line 7). However, there is no teaching or suggestion of any timewise association between the initial web purchase and the subsequent refresh requests, nor that the "periodically" (which, in view of the disclosure, is believed to mean occasionally or intermittently) generated requests are made at any particular times relative to each other. It is further submitted that such refresh request timing as recited in Claim 12, as amended, would not be necessary in Schmeidler because the separate on-demand downloads from different PCs would be naturally staggered, and there would be no traffic peak problems regardless. It is further noted that the refresh requests in Schmeidler are not for encryption keys "used to encrypt" or to "decrypt the multicast event," but rather for "RAFT tokens" that are submitted by the PC to the RAFT server (col. 14, lines 50-52) so that downloading of the content itself may continue.

Claims 13-18 are submitted to be allowable for at least the reason that they depend from an allowable base claim.

Claim 19

It is respectfully submitted that Claim 19, as amended, is patentable over Akins for reasons similar to those presented above in regard to Claim 1. For example, Akins does not teach or suggest "each key corresponding to a one of a plurality of time intervals that are relatively short compared to a duration of the multicast event" as recited in Claim 19, as amended. Various other minor amendments have been made to Claim 19 for further clarity, antecedent basis, etc.

Claims 20-21 are submitted to be allowable for at least the reason that they depend from an allowable base claim, and each has been amended for consistency with amended Claim 19.

Claim 22

It is respectfully submitted that Claim 22, as amended, is patentable over Akins for reasons similar to those presented above in regard to Claim 1. For example, Akins does not teach or suggest "the key being refreshed at relatively short intervals compared to a duration of the multicast event" as recited in Claim 22, as amended.

Claims 23-28 are submitted to be allowable for at least the reason that they depend from an allowable base claim.

Claim 29

It is respectfully submitted that Claim 29, as amended, is patentable over Akins for reasons similar to those presented above in regard to Claim 1. For example, Akins does not teach or suggest "the symmetric key being refreshed at relatively short intervals compared to a duration of the multicast event, the refreshed symmetric keys being transmitted from the key server to said receiving client during the multicast event" as recited in Claim 29, as amended.

Claim 30

It is respectfully submitted that Claim 30, as amended, is patentable over Akins for reasons similar to those presented above in regard to Claim 1. For example, Akins does not teach or suggest "the symmetric key being refreshed at relatively short intervals compared to a duration of the multicast event, the refreshed symmetric keys being transmitted from the key server to said receiving client during the multicast event" as recited in Claim 30, as amended.

Claim 31 was not rejected under 35 USC 103(a). See above discussion of 35 USC 112 Rejections.

Claim 32

It is respectfully submitted that Claim 32, as amended, is patentable over Akins for reasons similar to those presented above in regard to Claim 1. For example, Akins does not teach or suggest "the symmetric key being refreshed at relatively short intervals compared to a duration of the multicast event, the refreshed symmetric keys being transmitted from the key server to said receiving client during the multicast event" as recited in Claim 32, as amended.

Claim 33 is submitted to be allowable for at least the reason that it depends from an allowable base claim. Furthermore, it could not be found in the Akins portions cited in the Office Action (cols. 4-5, col. 22, lines 30-60, col. 23, col. 27, lines 1-10) "wherein the list comprises . . . an internet protocol (IP) address for each listed event . . . and an IP address for a key server

corresponding to each listed multicast event.” Instead, as understood, Akins discusses a cable TV distribution system. The set-top box only gets content that passes through the “headend 515.”

Claim 34 is submitted to be allowable for reasons similar to those presented above with respect to Claim 12.

Claims 35-38 are canceled herein without prejudice or disclaimer.

Claim 39 is submitted to be allowable for reasons similar to those presented above with respect to Claim 12.

Claims 40-41 are canceled herein without prejudice or disclaimer.

Claim 42 is submitted to be allowable for reasons similar to those presented above with respect to Claim 12.

Claims 43-48 are submitted to be allowable for at least the reason that they depend from an allowable base claim.

Appln. No. 09/544,898
Amdt./Response submitted Jan. 31, 2005,
Reply to Office Action of Aug. 30, 2004

PATENT
Customer No. 22,852
Attorney Docket No. 7451.0032-00
Intertrust Ref. No. IT-48 (US)

CONCLUSION


In view of the foregoing remarks, Applicants submit that this claimed invention is allowable over the references cited against this application. Applicants therefore request the entry of this Amendment, reconsideration and reexamination of the application, and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916 .

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: January 31, 2005

By: 
Andrew B. Schwaab
Reg. No. 38,611

Finnegan Henderson Farabow
Garrett & Dunner LLP
901 New York Avenue, NW
Washington, D.C. 20001-4413
(202) 408-4000